# QUANTUM INFORMATION, COMPUTATION AND FUNDAMENTAL LIMITATION

Arun K. Pati
Theoretical Physics Division

## Introduction

Quantum information theory is a marriage between two scientific pillars of the twentieth century science, namely, quantum theory and classical information theory. Quantum theory as developed by Planck, Einstein, Schrodinger, Dirac, Heisenberg, and many others in early part of the last century is one of the finest theories that explains phenomena ranging from molecules to electrons, protons, neutrons and other micro particles. Mathematical theory of classical information was also propounded by C. Shannon in the midpart of the last century. Whatever revolution in information technology we see at present is partly due to the ground-breaking work by C. Shannon, A. Turing, A. Church and many others.

When the ideas from classical information theory are carried over to quantum theory there emerges a revolution in our ability to process information. The very basic ways of expressing and manipulating information require physical states and processes. In quantum theory we know that the physical processes are fundamentally different than those of classical physics. Therefore manipulation of information based on quantum physical processes has to be also fundamentally different than their classical counterparts [R. Feynman, *Found. of Physics* 16 (1986) 507]. It is this urge to understand what we can do with the new ways of expressing information, which has led to several surprising discoveries in last two decades or so. The subject of Quantum Information is quite vast, and very broadly deals with topics such as Quantum Computing, Quantum Cryptography, Quantum Entanglement, New protocols for information processing and many more tasks which cannot be achieved classically [see for example: A. Zeilinger, *Phys. World* (March), 35-40 (1998)]. Here, we plan to give a brief overview of recent excitement in quantum computation and some fundamental limitations on quantum information.

## Quantum Computation

Physics of information and computation are intimately related. Information is encoded in a state of a physical system. Computation is processing of information on actual physical system that obeys certain laws. Therefore, the study of information and computation are linked through a study of underlying physical processes. If the physical processes obey the rules of classical physics, the corresponding computation is classical. If the underlying processes are subjected to quantum mechanical rules, the resulting computation will be "*quantum computation*". The logic that lies at the heart of ordinary computers and quantum computers is completely direct. Quantum computation is a particular way of processing information which utilises principle of linear superposition, quantum entanglement and quantum measurement.

In conventional computers (present-day-computers) information is stored in bits such as 0's or 1's. To represent a bit, i.e., 0 or 1 one can use any physical system like a voltage in a circuit is at zero or at a positive bias, or current in a circuit in positive or negative direction, or by saying that a switch is on or off. A two bit information can be in any one of the $2^2 = 4$ possible states (e.g.00; 01; 10; 11). A three bit information can be in any one of the $2^3 = 8$ possible logical states (e.g. 000; 111; 011; 110; 101; 001; 100; 010). An $n$ bit information can exist in any one of the $2^n$ possible logical states one at a time. Information stored in these binary digits can be manipulated using elementary logic gates that obey Boolean algebra. For example, in a classical computers one can manipulate information using sequence of logical operations such as AND, OR, NOT, and XOR gates. Computations that are done in our desk top computers basically use these logic gates.

### *Quantum Bit or Qubit*

Suppose we represent a bit 0 or 1 by saying that the spin of a neutron is up or down, or we could say an atom is in ground or in an excited state, or a photon is horizontally or vertically polarized. All these systems are called two-state quantum systems because they can remain in any of these two logical states. Therefore, when a photon is in a defnite polarization state it carries classical information (as it represents a 0 or a 1). However, quantum theory also allows a state of a spin-half particle, which is in a linear combination of spin up and down. This implies a new possibility for representing information by a two-state quantum system which can be both 0 and 1, i.e., a state of the type $\alpha|0\rangle + \beta|1\rangle$ with $\alpha$ and $\beta$ being complex numbers in general and $|\alpha|^2 + |\beta|^2 = 1$. (According to Dirac a quantum state is denoted by a ket $|\cdot\cdot\rangle$, which for a two-state system is a column matrix with two entries). This is called a quantum bit or `qubit'. As we will see in subsequent section an arbitrary qubit contains a large amount of information. It is possible to design several new type of logic gates acting on qubits which can perform many computational tasks in parallel (due to linear superposition principle) which cannot be realised with classical computers [D. Deutsch, Proc. R. Soc. London. A, 400, 97-117 (1985)]. One may recall that it is this linear superposition that lies at the heart of interference of quantum particles when they are made to pass through a Young's double slit experimental setup.

### *Quantum Register*

It is a collection of qubits on which a program is to be executed. For example, if we have two qubits, they can exist in four logical states 00; 01; 10 and 11 and they can also exist in a *linear superposition of all four logical states*. In the latter case a typical state will be $\alpha|00\rangle + \beta|01\rangle + \delta|10\rangle + \gamma|11\rangle$. If there are *n* qubits they can exist in any one of the $2^n$ possible logical states and also can exist in a linear superposition of all $2^n$ logical states. This latter property in case of two or more quantum systems can give rise to quantum entanglement (inter-twinedness). A composite state is entangled if it is not a product of individual states. A simplest example of entangled state is Einstein-Podolsky-Rosen state $1/\sqrt{2}(|01\rangle - |10\rangle)$ for two qubits which is familiar spin-singlet for two spin-half particles. In this state there is equal probability of finding the spins (ups and downs) for two qubits. Further, if spin of one particle is found up then the other is in down state. If two particles are in an entangled states then measuring one will affect the other instantaneously even though they are far separated in space. Spatial distance is immaterial because there is correlation in internal degrees of freedom. One can imagine that `somehow' two particles love so much that even if they are far apart, still they are in contact! Physicists are still trying to understand the mechanism of this `somehow'.

### *Quantum Parallelism and Quantum Algorithm*

Like in a classical computer, to run a program in a quantum computer (QC) algorithms have to be devised. Algorithms on a quantum computer can be implemented by sequential application of quantum logic gates, which are nothing, but a set of unitary operations on n quits. An important result in this area is that any arbitrary operation ($2^n \times 2^n$ matrix) on n-qubits can be designed from single-qubit operator (2 x 2 matrix) and two-qubit operators (4 x 4 matrix).

The striking feature of QC is its computational potential – called “quantum parallelism". Suppose there is a black box that computes a function from an input bit x; (x = 0; 1; …. $2^n$ ), i.e., it takes a single bit x to a single bit f(x). Classically one has to do $N=2^n$ function evaluations. But quantum mechanically all the N function evaluation can be done in one go because a QC can remain in a superposition of all N possible logical states (see fig 1). However, to know the answer we have to do a measurement on the output register and that will destroy the coherence. The result will be obtained according to certain probabilities. Thus it is a highly non-trivial task to design a quantum computer and get an answer for a desired problem.

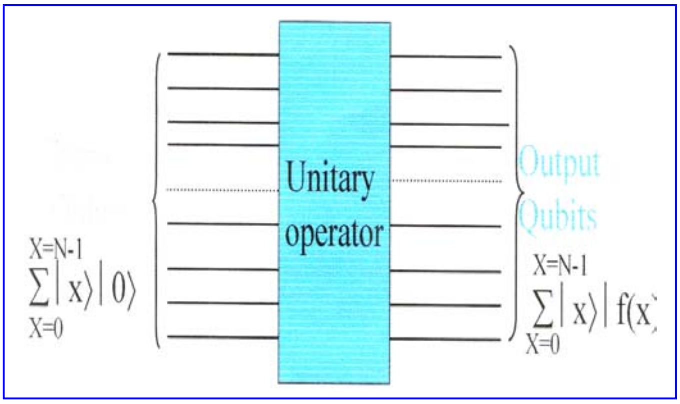


*Fig.1 Parallelism in quantum computing: if a unitary operator U takes* $|x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle$, *with x=0,1,.....N, then a single action of U on equal superposition of logic states evaluates the function for all possible inputs of x.*

But why is it so interesting? It is not that a QC can solve some problem which cannot be solved in a classical computer (though this question is still an open). A quantum computer can solve all those problems that can be done on a classical computer. In addition, it can solve computationally hard problems with ease. 'Computationally hard' is measured through computational complexity – which says how the number of steps *s* required in a computation scales with the size of the input. If we feed an input number *N,* the information or length of the input is $L = \log_2 N$. If *s* is a polynomial function of *L* (such as say $s \approx aL + bL^2$ ), then the problem is tractable and if *s* grows exponentially with *L* (such as say $s \approx \exp[f(L)]$, where *f(L)* is some non-exponential function of *L),* then the problem is `hard'.

In recent years there have been three important algorithms discovered. One is the Deutsch-Josza (DJ) algorithm where one aims to know some `global' information about a binary function *f(x),* i.e., to know whether the function is balanced or constant. A balanced function is one which is 0 for half of the case and 1 for other half or vice versa. A constant function is one which is either 0 or 1 for all values of *x*. Since *x* takes *N* possible values a classical computer will take O(N) steps to decide it. But Deutsch and Jozsa found an algorithm on a quantum computer which can decide it in one step! So there is an exponential speed-up in a quantum computer [D. Deutsch and R. Jozsa, *Proc. R. Society (London),* Ser. A **439** (1992) 553]. The second is the Shor algorithm where one aims to factorise a composite (a non-prime) number *x*. In general it is an intractable problem. In a classical computer the best known algorithm takes an exponentially large number of steps. Shor discovered that a QC can do the job in a polynomial number of steps. For example, to factor a number of size *L ~ 600,* the number of steps it takes is $s \sim 10^{25}$. It will take million years in a classical superfast computer but a quantum computer can do the factorisation in $s \sim 10^8$ steps, i.e., in few seconds! Shor's algorithm is one of the land-mark papers in quantum computation that generated a widespread interest among physicists, computer scientists, mathematicians and others alike [P. Shor, *Proc. 35th Annual Symp. on Found. of Comp. Sci.* IEEE Computer Society Press, 1994]. The third is the Grover algorithm, where one aims to find one particular item from a large unsorted data base containing *N* items. Classically, one needs to search *O(N)* times to find a particular item but quantum mechanically one can search in $O(\sqrt{N})$ steps [L. K. Grover, *Phys. Rev. Lett.* 79 (1997) 325]. There is a square-root improvement (i.e., the speed-up is polynomial) which can be a great advantage for large data base searches. For example, to find a person's name in a directory containing $10^8$ entries, a classical computer will take so many steps whereas a quantum computer can do only in $10^4$ steps.

These discoveries are important not only for physicists but also for computer scientists because they provide radical way of thinking about computation, information, and programming in general. It is worth mentioning that DJ's and Grover's algorithms have been implemented on `primitive quantum computers'. There have been various proposals to build a quantum computer but a full scale QC is far from scene. The experimental proposals include isolating and manipulating qubits in ion traps, solid state based devices such as SQUIDS, quantum dots, NMR techniques and many more [see for latest progress in experimental QC: *"Scalable Quantum Computers"* by H. K. Lo and S. L. Braunstein (Eds), Wiley-VCH Publisher, 2000].

## Fundamental Limitations on Quantum Information

As we have discussed, qantum computation is a certain way of processing quantum information to achieve startling speed-ups in some class of problems. But there are much more amazing tasks one can do with quantum information. On the other hand there are some limitations on quantum information too. Therefore, it is important to know what type of operations are allowed in quantum world and what are not. These limitations are sign posts on the progress road of quantum information. In future when we build quantum information processing units we would know what type of machines we need to design.

### *Knowledge of a Quantum state*

Quantum information has certain unique properties, which distinguish it from their classical counterpart. The *'knowledge*' of a quantum state is very crucial in deciding what operations one can do and what cannot. There is a vast difference between the information content of a quantum state being 'known' and `unknown'. But classically the information about a state can be known in principle. We know that in classical world the state of a particle is described by its position and momentum and there are no fundamental limitations on the precision with which we can measure these variables. Therefore, even if we do not know the state of a classical particle, we can always design an apparatus which can measure its state precisely without disturbing the particle. However, in the quantum world a state of a particle is not described by its position and momentum but by a wavefunction (in abstract 4 notion it is a state vector in a complex, linear, complete vector space called a Hilbert space). An important question is can we `know' the state of a particle if we are given just a single quantum system? The answer is `no'. To determine the state of a system completely one needs infinite number of identically prepared particles. For example, for a qubit described by a state $|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle$, if we say '*we know the state*' – this means, we know precisely the value of $\theta$ and $\phi$ (see fig. 2).

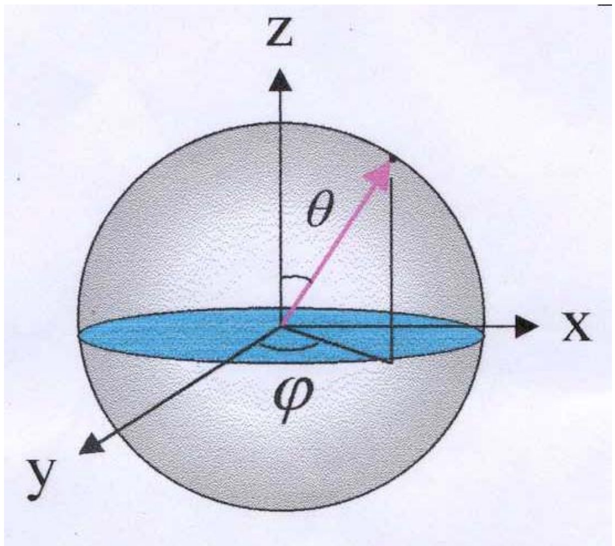


*Fig 2. Geometrical way of representing a qubit on a Bloch sphere. All the points on this sphere represent possible states of a qubit. The tip of the arrow representing the point is a qubit parametrised by polar angle $\theta$ and azimuthal angle $\varphi$.*

That is to say we `*know*' the exact point on the Bloch sphere. This is possible only when we have prepared the qubit ourselves by a suitable machine. But if some one else has prepared the qubit and given it to us, then the qubit is `*unknown*' to us. What it means is that we do not know the value of two real parameters $\theta$ and $\phi$, and if we do not know them, there can be infinite number of possible value that they can assume. In other words if we do not know the exact point on the Bloch sphere, the point can lie any where (which has infinite number of possibilities). Therefore, *to specify an unknown qubit one needs infinite number of bits* (which is nothing but logarithm of number of possibilities). On the other hand we do not need any extra bits to specify a *known* qubit, because we have the complete knowledge (i.e. we do not lack any information).

One may wonder is it not possible to extract the information about the unknown numbers $\theta$ and $\phi$ by measurement? But if one performs measurements on a qubit one will get only two possible outcomes, i.e., it will project either to $|0\rangle$ or $|1\rangle$ with probability $\cos^2\frac{\theta}{2}$ and $\sin^2\frac{\theta}{2}$, respectively. Therefore, one can extract only one bit of information ($\log_2 2 = 1$) by a measurement! Moreover, after a measurement the state of the qubit is no longer the same. It has irreversibly changed to one of the two distinct states. This is a riddle of quntum information: even though an unknown qubit contains infinite amount of bits one can extract only one bit of information. Surprisingly, this *'unknowability'* of a quantum state has important implications in quantum information processing. It is precisely this nature of a quantum object that prohibits us to copy a quantum state, to delete a copy from two copies or to  a state to its orthogonal state and many more.

### *No-cloning principle*

We know that in classical world all information can be copied perfectly. A pedagogical (but crude) example is an ordinary xerox machine, where we feed a page containing some classical information and few blank sheets at input port and at the output port we get two or more copies. The xerox machine is `universal' in the sense whatever information you feed you will get exact copies of an input. Moreover, the company which has designed a xerox machine does not know what information we will be copying. This means the information at users hand is apparently unknown to the person who has designed a xerox machine. Yet, it works equally well for all classical information. This is one example, which shows that in the classical world it possible to produce exact copies (in fact as many as we want) of any information. The other example is in a conventional computer we can always copy bits of information. This can again be done by designing suitable logic gates such as controlled NOT (CNOT) gates. A CNOT gate, for example, takes two bits as an input and produced two bits at the output such that the second bit is flipped if and only if the first bit is 1 (i.e.; 00 $\to$ 00; 01 $\to$ 01; 10 $\to$ 11; 11 $\to$ 10). Take 0 and 1 as inputs and 0 as a blank bit then by applying CNOT one can get 00 $\to$ 00 and 10 $\to$ 11, which is a copying operation. Everybody is familiar with making copies of some files in an ordinary computer.

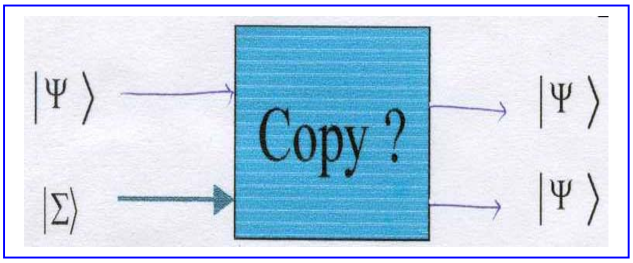


*Fig.3  Quantum xerox machine*

But can one design a xerox machine for a quantum state that will produce an exact copy of an `*unknown*' state? Surprisingly the answer is no. *We cannot copy an unknown quantum state!* This is a consequence of linearity of quantum evolution discovered by Wootters, Zurek and Dieks [W. K. Wootters and W. H. Zurek, Nature 299 (1982) 802; D. Dieks*, Phys. Lett. A* 92 (1982) 271]. In quantum worlds copying process for an `unknown' qubit would involve the following action $|\Psi\rangle|\Sigma\rangle \to |\Psi\rangle|\Psi\rangle$, where $|\Psi\rangle$ is the state of the qubit, $|\Sigma\rangle$ is the blank state (analogous to blank paper in a xerox machine, see fig. 3).

If a qubit is in any one of the orthogonal state $|0\rangle$ or $|1\rangle$ , then it carries classical information and one can design a xerox machine that can copy it perfectly. For example, a photon in a horizontal or vertical polarization state can be copied perfectly. But when a qubit is in an arbitrary linear superposition of two distinct bits then the machine fails. However, if we `*know*' a qubit we can copy it perfectly. No-cloning principle is in agreement with established principles. For example, if we could clone an unknown state perfectly then by making two sets of identical ensembles one can measure position on one and momentum on the other precisely. This will allow us to measure two conjugate properties of a system, which, in turn violates Heisenberg's uncertainty relation. Moreover, if we can clone an arbitrary state then using spin-singlet entangled state one can send signals faster than light. Because Alice at one end can measure her particle onto two orthogonal basis (she can get 1 bit) and Bob at the other end can use a cloning machine to produce infinite number of copies of his particle and can infer the measurement out come of Alice. This will allow a communication of 1 bit faster than light. But we know that we cannot send signals faster than light and this is another reason why cloning of `unknown' states must be an impossible operation.

***No-deletion principle***

Yet, another fundamental limitation on quantum information has been discovered recently. In classical information theory deleting copies of some information is always possible using a CNOT gate. However, in quantum theory the perfect deletion of an unknown state from a collection of two copies is an impossible operation [A. K. Pati and S. L. Braunstein, *Nature* 404 (2000) 164]. To understand this question better imagine that there are two persons Alice and Bob. Alice prepares two copies of a qubit and gives to Bob. Now the information about the qubit is *known* to Alice but *unknown* to Bob. Then Alice asks Bob to design a deletion machine. Can Bob design *a* all purpose deletion machine? Not so. The very basic structure of quantum theory puts strong limitations on the complete deleting of the quantum information of an *unknown* state.

Here one should distinguish the process of erasure from deletion. Classically, erasure refers to getting rid of last bit of information from a collection of *unordered bits* whereas deletion refers to resetting the last bit to a standard bit from a collection of *identical ordered bits*. Classical deletion takes an ordered set of bits to another ordered set of bits and this is logically reversible. But erasure is an irreversible operation. In classical information theory there is Landauer's principle of erasure, which says that if you throw away one bit of information it must dissipate energy $E = kT \log 2$ at temperature $T$. Thus erasure of a single bit leads to increase of entropy of the surrounding by an amount $k \log 2$.


*Fig. 4 Quantum deleting machine*

The quantum deletion is fundamentally different than erasure [W. H. Zurek, *Nature*, 404 (2000) 130]. Quantum deletion as defined aims to create a blank state and original copy states from two copies by a linear operation acting jointly on all the copies. For example the deletion process would take two copies of an unknown neutron or photon and produce a blank state together with the original copy. If we have two photons with arbitrary polarisation in some state $|\Psi\rangle$, the action of deleting machine can be represented as (see fig.4) $|\Psi\rangle|\Psi\rangle \rightarrow |\Psi\rangle|\Sigma\rangle$.

It was proved that though the above machine can work for qubits in orthogonal states but for an arbitrary qubit the above process does not exist. By linearity one can show that the final output states are different in ideal case and actual case. *Therefore linearity does not allow deleting of an unknown quantum state against a copy*. This principle is now called “quantum no-deletion" principle. Nevertheless, if one knows a qubit one can delete a copy. This is not just reverse of no-cloning principle, but an independent principle by itself. It is worth mentioning that in classically world one can erase and delete information (both the operations are allowed) but in quantum world one *cannot delete* but can only *erase* information at some energy cost.

The important implication of no-cloning which was discovered some twenty years ago is realised in recent years. Similarly, the implication of no-deleting principle discovered only last year will be realised in times to come. It is a hope that this may have some applications in the quantum computer and in general other quantum information processing units.

***No-flipping principle***

We know that classical information consisting of bits such as 0 or 1 can be  i.e., 0 goes 1 and 1 goes to 0. This can be achieved by a using a NOT gate. Similarly, in quantum world a qubit in a prefered logical state $|0\rangle$ or $|1\rangle$ can be flipped because they again carry classical information. But can one flip an *unknown* qubit which is in an arbitrary superposition of two distinct logical states? Operationally, one can represent the flipping action as $|\Psi\rangle \rightarrow |\overline{\Psi}\rangle$, where $|\overline{\Psi}\rangle$ is orthogonal to $|\Psi\rangle$.

The answer to the above question is again 'no'. The reason behind such an impossibility is that we do not know the exact location of the point on the Bloch sphere. The flipping operation is nothing but inversion of the Bloch sphere. If we know the qubit, then we know the exact location of the point on the Bloch sphere and we can apply a rotation operator to get the flipped state. When the point on the Bloch sphere is unknown we cannot chose the NOT gate appropriately. Therefore an unknown qubit cannot be  i.e., there is no universal-NOT gate for a qubit [V. Buzek, M. Hillery and R. F. Werner, *Phys. Rev.* A **60** (1999) R2626]. Surprisingly, if one picks up qubits from equatorial or polar great circles on a Bloch sphere then it is possible to design a NOT gate. This means that any point from these special class of states can be flipped exactly. With a priori information about qubits, even if they are unknown still they can be  flipped exactly [A. K. Pati, *Phys. Rev.* A **63** (2001) 014302].

The physical reason behind such impossible operations is traced to our `ignorance' about the qubit. This quantum ignorance is not just a practical one but of *fundamental one which cannot be removed at any cost.* However, the classical ignorance can always be removed in principle by suitable measurements. Hence, there are no limitations on copying, deleting or  of classical bits.

## Applications

The impossibility of `knowing' a quantum state has important applications in *quantum cryptography.* Cryptography is an art of sending secret information between two parties. Usually, the security of classical cryptographic protocol depends on unproven assumptions about complexity of the retrieving the key. Bennett and Brasard [ C. H. Bennett and G. Brasard, *Proceedings of the IEEE Conf. on Computers, Systems and Signal Processing,* Bangalore, India: IEEE, 1984, 175] were the first to realise that by encoding bits in quantum states Alice can send confidential information to Bob. A third party Eve, cannot know what message is sent from Alice to Bob because she cannot know the quantum state completely, nor can she make copies of the quantum states. In case she tries to read the information by measurement there will be unavoidable disturbances in the message and Bob will come to know that there was a spy! So the security to cryptography is provided by no-cloning principle and the laws of quantum mechanics. Quantum cryptography may play an important role in defence applications such as sending secret information across boarder regions where absolute security is essential.

Quantum information processing is not only limited to quantum computation, quantum cryptography but many other protocols which are impossible classically. Some of those are quantum teleportation (a method to send an object without physically sending it but the cost of destroying the original), entanglement swapping (a method to create quantum entanglement between two particles which have never interacted), remote state preparation (a method to prepare certain class of qubit at a distant laboratory), and so on. In recent years considerable progress has been made by leading scientists all over the world (though in India it is yet to gain momentum). The future challenge lies in discovering new quantum algorithms, new limitations, and building quantum information processors that will ultimately transform the living style of human civilisation in twentyfirst century and the society as a whole.